日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: ２０００年　６月３０日

出願番号
Application Number: 特願２０００－１９８４２０

出願人
Applicant (s): 沖電気工業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　１月１２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１１１８０３

【書類名】　特許願
【整理番号】　SA003538
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/16
H04L 12/24
【発明者】
【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
【氏名】　小山　法孝
【特許出願人】
【識別番号】　000000295
【氏名又は名称】　沖電気工業株式会社
【代理人】
【識別番号】　100082050
【弁理士】
【氏名又は名称】　佐藤　幸男
【手数料の表示】
【予納台帳番号】　058104
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9100477
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　オブジェクト提供装置

【特許請求の範囲】

【請求項１】　認証の対象であるプリンシパルからの要求に応じて、オブジェクトを提供するオブジェクト提供装置であって、

前記プリンシパルに関する情報を記憶するプリンシパル情報記憶部と、

前記プリンシパルに関する情報と前記オブジェクトとの関係、及び前記オブジェクトを記憶するオブジェクト情報記憶部と、

前記プリンシパルを認証するための情報を前記クライアント装置から受信する受信部と、

前記受信部が受信したプリンシパルを認証するための情報に基づき、前記プリンシパル情報記憶部に記憶された前記プリンシパルに関する情報を参照することにより前記プリンシパルを認証する認証部と、

前記認証部により認証されたプリンシパルに関する情報を前記プリンシパル情報記憶部から読み出し、該読み出したプリンシパル情報に対応するオブジェクトを前記オブジェクト情報記憶部から読み出すアプリケーション部とを備えることを特徴とするオブジェクト提供装置。

【請求項２】　請求項１記載のオブジェクト提供装置であって、

前記アプリケーション部は、複数のサービスを有し、

前記プリンシパル情報記憶部は、プリンシパル情報が変更されたときに該変更の旨の通知を希望するサービスを登録し、前記プリンシパル情報が変更されたときに、該変更の旨を前記登録されているサービスに通知することを特徴とするオブジェクト提供装置。

【請求項３】　請求項２記載のオブジェクト提供装置であって、

前記オブジェクト情報記憶部は、前記通知を受けたときに、該通知の内容に従って、オブジェクト情報の内容を変更することを特徴とするオブジェクト提供装置。

【請求項４】　請求項１記載のオブジェクト提供装置であって、

前記プリンシパルは、前記クライアント装置、前記クライアント装置を使用す

るユーザ、前記クライアント装置を構成するオブジェクト、及び前記クライアント装置である携帯端末のうちのいずれかであることを特徴とするオブジェクト提供装置。

【請求項５】　請求項１記載のオブジェクト提供装置であって、

前記プリンシパルに関する情報と前記オブジェクトとの関係は、適合ルールによって規定されることを特徴とするオブジェクト提供装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、分散処理システムにおけるオブジェクトを提供するオブジェクト提供装置に関する。

【０００２】

【従来の技術】

従来から、分散処理システムではそのセキュリティを維持すべく、プリンシパルを認証することが行われている。認証されたプリンシパルによる資源へのアクセスを制御する方法として、例えば、アクセス制御リストを用いる方法がある。このリストは、プリンシパルがアクセスする資源、その資源に関する処理（例えば、読み出し、書き込み、実行等）、その処理の許否等を示す。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来のシステムでは、アクセス制御の対象となる資源、処理、許否等が限定されるという問題があった。

【０００４】

【課題を解決するための手段】

上記の問題を解決するために、本発明によれば、認証の対象であるプリンシパルからの要求に応じて、オブジェクトを提供するオブジェクト提供装置は、プリンシパルに関する情報を記憶するプリンシパル情報記憶部と、プリンシパルに関する情報とオブジェクトとの関係、及びオブジェクトを記憶するオブジェクト情報記憶部と、プリンシパルを認証するための情報をクライアント装置から受信す

る受信部と、受信部が受信したプリンシパルを認証するための情報に基づき、プリンシパル情報記憶部に記憶されたプリンシパルに関する情報を参照することによりプリンシパルを認証する認証部と、認証部により認証されたプリンシパルに関する情報をプリンシパル情報記憶部から読み出し、読み出したプリンシパル情報に対応するオブジェクトをオブジェクト情報記憶部から読み出すアプリケーション部とを備える。

【０００５】

アプリケーション部は、複数のサービスを有し、プリンシパル情報記憶部は、プリンシパル情報が変更されたときに変更の旨の通知を希望するサービスを登録し、プリンシパル情報が変更されたときに、変更の旨を登録されているサービスに通知することが望ましい。さらに、オブジェクト情報記憶部は、通知を受けたときに、通知の内容に従って、オブジェクト情報の内容を変更することがより望ましい。

【０００６】

プリンシパルは、クライアント装置、クライアント装置を使用するユーザ、クライアント装置を構成するオブジェクト、及びクライアント装置である携帯端末のうちのいずれかであることが望ましい。

プリンシパルに関する情報とオブジェクトとの関係は、適合ルールによって規定されることが望ましい。

【０００７】

【発明の実施の形態】

本発明の実施の形態について説明する。実施の形態として、具体例の分散処理システムについて説明する。

図１は、具体例の分散処理システムの構成を示す図である。この分散処理システムは、主に、複数のクライアント装置１Ａ～１Ｃ、オブジェクト提供装置２、及び、それらの装置１Ａ～１Ｃ、２を互いに接続するネットワーク３から構成される。このシステムでは、オブジェクト提供装置２は、クライアント装置１Ａ～１Ｃに、ネットワーク３を介してオブジェクトを提供する。

【０００８】

クライアント装置１は、要求メッセージ３００を送出することにより、オブジェクト提供装置２にサービスによるオブジェクトの提供を求め、また、オブジェクト提供装置２は、この求めに応じてオブジェクトを提供する。

【０００９】

このような機能を果たすべく、クライアント装置１Ａ～１Ｃのそれぞれは、ネットワーク通信管理部１０、及びクライアントアプリケーション部１１を備える。また、オブジェクト提供装置２は、ネットワーク通信管理部２０、ユーザ認証部２１、アプリケーション部２２Ａ、アプリケーション部２２Ｂ、プリンシパル情報管理部２３、プリンシパル情報管理インタフェース部２４、オブジェクト情報管理部２５、及びオブジェクト情報管理インタフェース部２６を備える。

【００１０】

各クライアント装置１では、ネットワーク通信管理部１０は、オブジェクト提供装置２との間でオブジェクトの授受を行うべく、オブジェクト提供装置２内のネットワーク通信管理部２０と通信を行う。クライアントアプリケーション部１１は、オブジェクトを授受すべく、クライアント装置１Ａ～１Ｃのユーザによって操作される。

【００１１】

オブジェクト提供装置２では、ネットワーク通信管理部２０は、各クライアント装置１との間で通信を行い、例えば、クライアント装置１Ａから要求メッセージ３００を受信する。ユーザ認証部２１は、要求メッセージ３００に含まれる認証用データと、プリンシパル情報管理部２３に予め登録された認証用データとを比較することにより、ユーザを認証する。

【００１２】

アプリケーション部２２Ａ、２２Ｂは、複数のサービス２００Ａ、２００Ｂ、２００Ｃ、及び２００Ｄを有し、また、プリンシパル情報管理部２３やオブジェクト情報管理部２５へのアクセスを互いに独立して行う。

【００１３】

プリンシパル情報管理部２３は、プリンシパルの管理やプリンシパルに関する情報の管理を行う。より具体的には、プリンシパルの登録、削除、参照やプリン

シパル情報の設定、取得、削除、参照等を行い、そのために、プリンシパル情報管理インタフェース部２４を有する。ここで、プリンシパルとは、ユーザ、クライアント装置、クライアント装置を構成する構成要素、携帯端末等の主体をいう。

【００１４】

オブジェクト情報管理部２５は、プリンシパル情報とオブジェクトとの対応を管理する。より具体的には、オブジェクトを記憶し、また、例えば、アクセス制御や処理制御等の制御のために用いる、プリンシパル情報とオブジェクトとの対応関係を管理する。このような管理のために、オブジェクト情報管理部２５は、オブジェクト情報管理インタフェース部２６を有する。

【００１５】

図２は、プリンシパル情報及びオブジェクト情報の管理・操作を示す構成図である。同図に示されるように、プリンシパル情報管理部２３は、ＡＰ部２３０、管理部２３１、及び記憶部２３２を含む。オブジェクト情報管理部２５もまた、ＡＰ部２５０、管理部２５１、及び記憶部２５２を含む。

【００１６】

上位層に位置するＡＰ部２３０、２５０は、プリンシパル情報やオブジェクト情報がアプリケーション部２２毎に規定されることから、アプリケーション部２２に依存する。下位層に位置する記憶部２３２、２５２は、それぞれ、プリンシパル情報及びオブジェクト情報を記憶する。

【００１７】

中間層に位置する管理部２３１、２５１は、アプリケーション部２２に依存することなく、全てのアプリケーション部２２によって共通して利用されることができる。管理部２３１は、イベントリスナとしてサービスを登録し、その登録されたサービスへイベントの発生を通知すべく、イベントリスナを管理するためのテーブル４００を記憶する。

【００１８】

図３は、プリンシパル情報管理部内の管理部の動作を示す図である。管理部２３１は、各コマンドを入力されることにより、対応する処理を返す。より詳しく

は、addAPは、アプリケーション部２２の追加、removeAPは、アプリケーション部２２の削除、listAPは、アプリケーション部２２の一覧、addPrincipalは、プリンシパルの追加、removePrincipalは、プリンシパルの削除、getPrincipalInfoは、プリンシパルの一覧の表示、removePrincipalInfoは、プリンシパル情報の追加、listPrincipalInfoは、プリンシパル情報の取得、addEventListenerは、プリンシパル情報の変更時にイベントを受信するリスナの追加、removeEventListerは、リスナの削除、listEventListenerは、リスナの一覧の表示を意味する。

【００１９】

図４は、オブジェクト情報管理部内の管理部の動作を示す図である。管理部２５１は、各コマンドを入力されることにより、対応する処理を返す。より詳しくは、addAPは、アプリケーション部２２の追加、removeAPは、アプリケーション部２２の削除、listAPは、アプリケーション部２２の一覧の表示、addKeyは、キーの追加、removeKeyは、キーの削除、listKeyは、キーの一覧の表示、putObjectInfoは、オブジェクト情報の追加、getObjectInfoが、オブジェクト情報の取得、removeObjectInfoは、オブジェクト情報の削除、listObjctInfoは、オブジェクト情報の一覧の表示を意味する。なお、principalInfoValueTemplateは、オブジェクトを取得するときの適合ルールである。

なお、オブジェクト提供装置２の各部は、オブジェクトの提供に関し、機能単位で互いに独立して機能し、これにより分散処理システムとして機能する。

【００２０】

図５は、具体例の分散処理システムの動作を示すフローチャートである。以下、このフローチャートに沿ってその動作を説明する。説明及び理解を容易にすべく、クライアント装置１Ａのユーザがオブジェクト提供装置２から自己の年齢、性別に対応する配布物を受け取る例について説明する。動作の説明に先立ち、プリンシパル情報管理部２３及びオブジェクト情報管理部２５に記憶された情報について説明する。

【００２１】

図６は、プリンシパル情報管理部に記憶された情報を示す図である。同図に示されるように、プリンシパル情報管理部２３は、アプリケーションＩＤ、プリン

シパルＩＤ、及び、プリンシパル情報を記憶する。プリンシパル情報は、プリンシパル情報キー及びプリンシパル情報値から構成される。より具体的には、アプリケーションＩＤとして、「delivery」を記憶し、プリンシパルＩＤとして「sakurai123」を記憶し、プリンシパル情報キーとして「PersonalData」を記憶し、プリンシパル情報値として「{1970/1/1,“man”}」を記憶する。

【００２２】

図７は、オブジェクト情報管理部に記憶された情報を示す図である。同図に示されるように、オブジェクト情報管理部２５は、アプリケーションＩＤ、キー、及びオブジェクト情報を記憶する。オブジェクト情報は、オブジェクト情報キー及びオブジェクト情報値から構成され、さらに、オブジェクト情報キーは、プリンシパル情報キー及びプリンシパル情報値テンプレートから構成される。オブジェクト情報管理部２５は、より具体的には、アプリケーションＩＤとして、「delivery」を記憶し、キーとして「deliverItem」を記憶し、プリンシパル情報キーとして「PersonalData」を記憶し、プリンシパル情報キーとして「{30,“man”}」～「{20,“woman”}」を記憶し、オブジェクト情報値として「Ａ」～「Ｄ」を記憶する。プリンシパル情報キー「PersonalData」は、適合ルールを含み、その適合ルールは、例えば、今日の日付と生年月日との差、即ち年齢を算出することである。この年齢は、プリンシパル情報値テンプレートで検索するときに用いられる。

【００２３】

図５に戻って動作について説明する。

ステップＳ１００：ユーザは、クライアント装置１内のクライアントアプリケーション部１１により、サービス２００を受けるための操作を行う。それにより、ネットワーク通信管理部１０は、オブジェクト提供装置２へサービス２００を要求する要求メッセージ３００を送出する。要求メッセージ３００は、プリンシパルＩＤ、パスワード、コマンド等を含む。

【００２４】

ステップＳ１１０：オブジェクト提供装置２では、ネットワーク通信管理部１０が要求メッセージ３００を受信すると、ユーザ認証部２１は、要求メッセージ

中のパスワードに基づき、プリンシパル情報管理部２３を参照しつつ、ユーザを認証する。

【００２５】

ステップＳ１２０：ユーザが正規であると認められると、ユーザ認証部２１は、要求メッセージ３００をアプリケーション部２２に受け渡す。要求メッセージ３００を受け取ると、アプリケーション部２２は、要求メッセージ３００の内容に応じて、その要求メッセージ３００をサービス２００Ａ～２００Ｄのいずれかに振り分ける。即ち、要求メッセージ３００を処理すべきサービス２００を選択する。ここでは、要求メッセージ３００がサービス２００Ａに振り分けられたことを想定する。

なお、ユーザが正規であると認められないときには、オブジェクト提供装置２は、ユーザの認証に続く処理を一切実行しない。

【００２６】

ステップＳ１３０：サービス２００Ａは、要求メッセージ３００中のプリンシパルＩＤに基づき、そのプリンシパルＩＤに対応する情報をプリンシパル情報管理部２３から取得する。より具体的には、プリンシパル情報キー「PersonalData」やプリンシパル情報値「{1970/1/1, “man”}」を読み出す。

【００２７】

ステップＳ１４０：サービス２００Ａは、プリンシパル情報値「{1970/1/1, “man”}」、及び今日の日付「{2000/*/*}」を用いて、プリンシパル情報キー「PersonalData」に含まれる適合ルールに従うことにより値「{30, “man”}」を算出する。これにより、サービス２００Ａは、値「{30, “man”}」に対応するオブジェクト情報値「Ａ」、即ち、配布物「Ａ」を取得する。

【００２８】

ステップＳ１５０：配布物「Ａ」を取得すると、サービス２００Ａは、配布物「Ａ」をクライアント装置１へ送出する。このようにして、クライアント装置１Ａを利用するユーザのプリンシパル情報値「{1970/1/1, “man”}」に対応するオブジェクトである配布物「Ａ」が、オブジェクト提供装置２からクライアント装置１Ａへ提供される。

【００２９】

図８は、プリンシパル情報が変更されときのサービス２００への通知を示すフローチャートである。以下、このフローチャートに沿ってその動作を説明する。説明及び理解を容易にすべく、プリンシパル情報キー「PersonalData」が使用されなくなることを想定する。この不使用の設定は、アプリケーション部２２を管理する管理者がプリンシパル情報管理インタフェース部２４を操作し、プリンシパル情報管理部２３からプリンシパル情報キー「PersonalData」を削除することにより行われる。

【００３０】

ステップＳ２００：複数のサービス２００Ａ～２００Ｄのうち、プリンシパル情報が変更されたときにその旨を示すイベントを通知されることを希望するサービス２００Ａ、２００Ｂは、プリンシパル情報管理部２３に変更の通知を求める。

ステップＳ２１０：通知を希望する旨を受け取ると、プリンシパル情報管理部２３は、サービス２００Ａ、２００Ｂを、図２に示されたテーブル４００にイベントリスナとして登録する。この結果として、プリンシパル情報管理部２３は、プリンシパル情報が変更されることを待つことになる。

【００３１】

図９は、イベントリスナを管理するテーブルを示す図である。同図に示されるように、サービス２００Ａは、アプリケーションＩＤ「delivery」、登録リスナ「listener Ａ」を登録される。また、同様にして、サービス２００Ｂもまた、アプリケーションＩＤ「delivery」、登録リスナ「listener Ｂ」を登録される。

【００３２】

ステップＳ２２０：上述の操作によりプリンシパル情報キー「PersonalData」がプリンシパル情報管理部２３から削除されると、プリンシパル情報管理部２３は、イベントリスナＡ、Ｂ、即ちサービス２００Ａ、２００Ｂに、その旨を通知する。これにより、サービス２００Ａ、２００Ｂは、プリンシパル情報キー「PersonalData」の削除を知得する。サービス２００Ａ、２００Ｂは、この削除に従

って、必要な処理、例えば、制御あるいは監視すべき資源の設定を変更する。

【００３３】

オブジェクト情報管理部２５もまた、通知を受け取る。通知を受け取ると、予め定められた処理に従って、プリンシパル情報キー「PersonalData」に関連するデータを削除する。

【００３４】

上述したように、具体例の分散処理システムによれば、サービス２００の提供を、プリンシパル情報及びオブジェクト情報を用いて管理することから、従来に比してサービス２００Ａ～２００Ｄの提供に汎用性を持たせることが可能になる。また、プリンシパル情報やオブジェクト情報を一元管理することから、複数のサービス２００Ａ～２００Ｄは、それらの情報を共通に使用することが可能になる。さらに、プリンシパル情報の変更をそのプリンシパルに関係するサービス２００Ａ、２００Ｂに通知することから、プリンシパルの変更を即時的にサービス２００Ａ、２００Ｂに反映させることが可能になる。

【図面の簡単な説明】

【図１】

具体例の分散処理システムの構成を示す図である。

【図２】

プリンシパル情報及びオブジェクト情報の管理・操作を示す構成図である。

【図３】

プリンシパル情報管理部内の管理部の動作を示す図である。

【図４】

オブジェクト情報管理部内の管理部の動作を示す図である。

【図５】

具体例の分散処理システムの動作を示すフローチャートである。

【図６】

プリンシパル情報管理部に記憶された情報を示す図である。

【図７】

オブジェクト情報管理部に記憶された情報を示す図である。

【図８】

プリンシパル情報が変更されたときのサービスへの通知を示すフローチャートである。

【図９】

イベントリスナを管理するテーブルを示す図である。

【符号の説明】

１Ａ～１Ｃ　クライアント装置

２　オブジェクト提供装置

３　ネットワーク

１０　ネットワーク通信管理部

１１　クライアントアプリケーション部

２０　ネットワーク通信管理部

２１　ユーザ認証部

２２Ａ、２２Ｂ　アプリケーション部

２３　プリンシパル情報管理部

２４　プリンシパル情報管理インタフェース部

２５　オブジェクト情報管理部

２６　オブジェクト情報管理インタフェース部

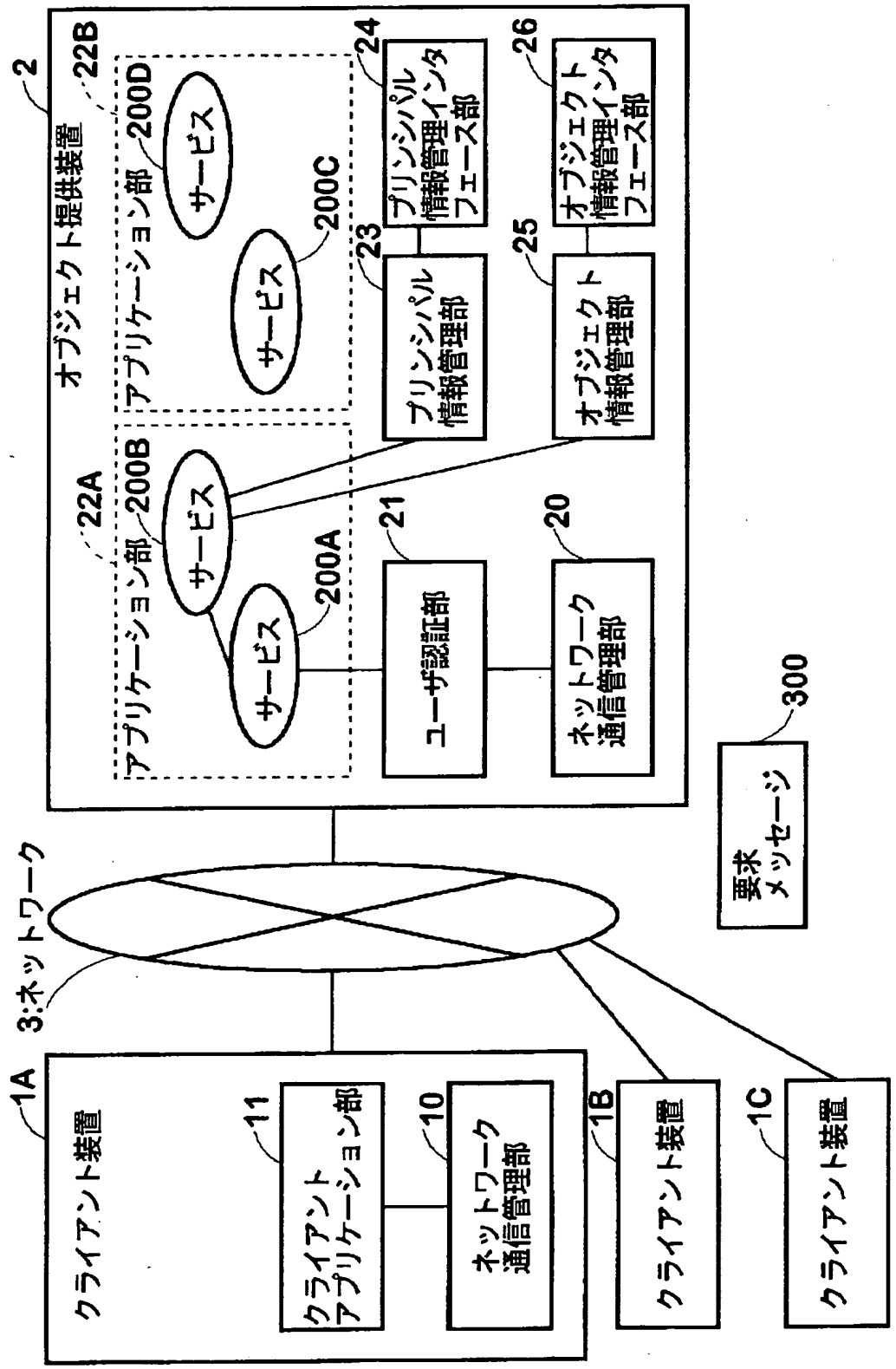
２００Ａ～２００Ｄ　サービス

３００　要求メッセージ

【書類名】図面

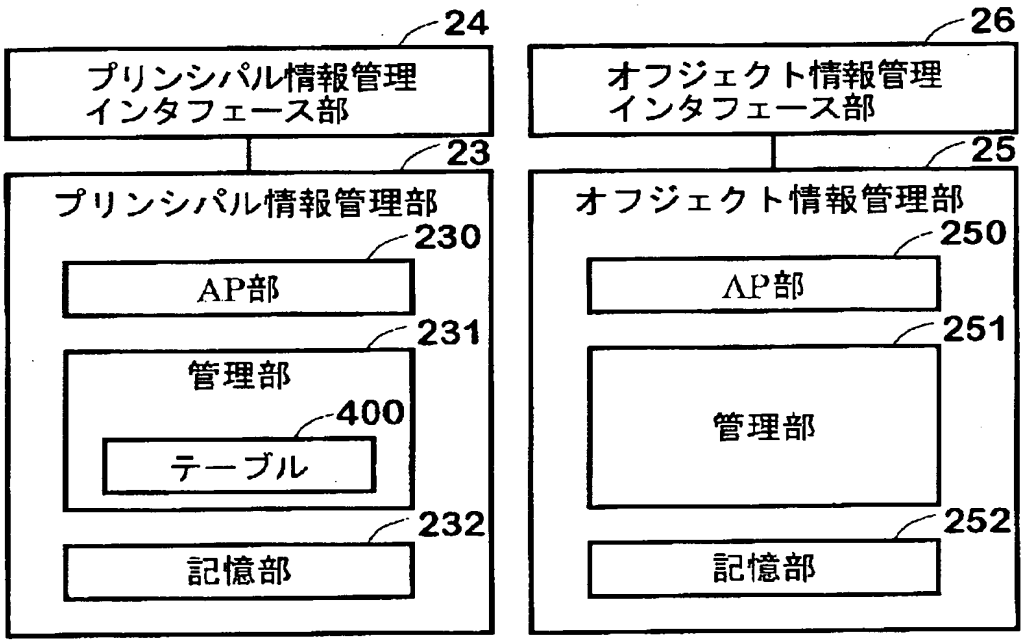
出証特２０００－３１１１８０３

【図１】



具体例の分散処理システムの構成を示す図

【図２】



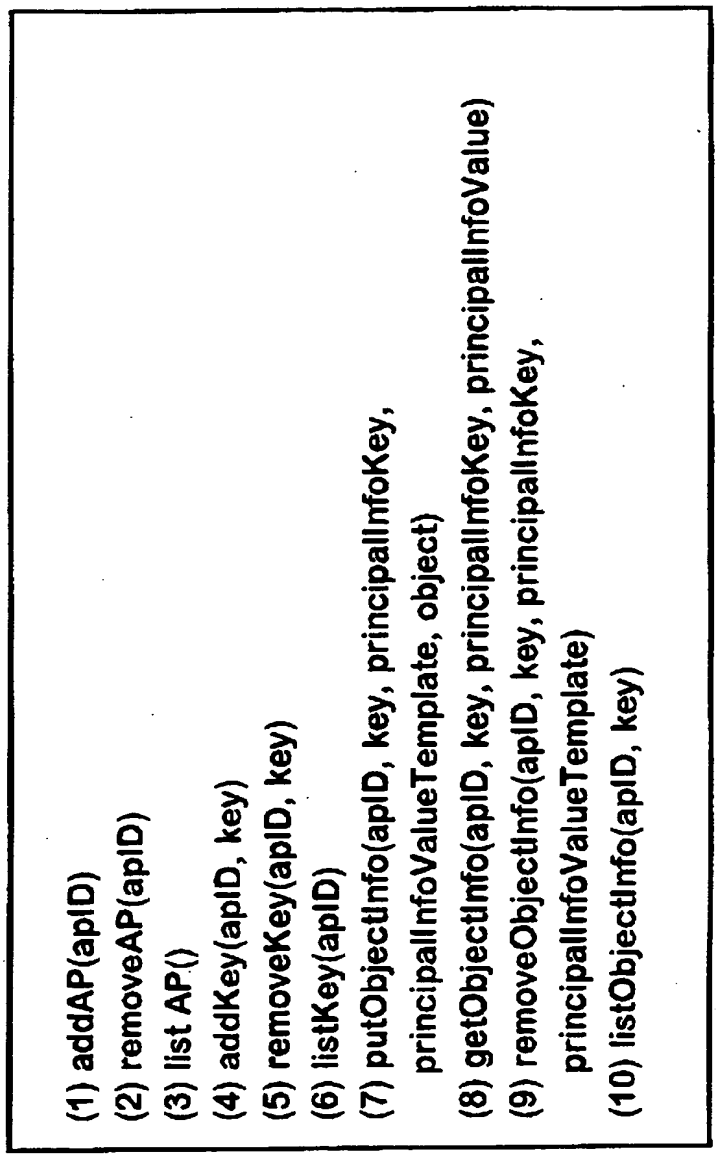
プリンシパル情報及びオブジェクト情報の管理・操作を示す構成図

【図３】

(1) addAP(apID)
(2) removeAP(apID)
(3) list AP()
(4) addPrincipal(apID, principalID)
(5) removePrincipal(apID, principalID)
(6) listPrincipal(apID)
(7) putPrincipalInfo(apID, principalID, principalInfoKey, principalInfoValue)
(8) getPrincipalInfo(apID, principalID, principalInfoKey)
(9) removePrincipalInfo(apID, principalID, principalInfoKey)
(10) listPrincipalInfo(apID, principalID)
(11) addEventListener(apID, listernerID, listener)
(12) removeEventListener(apID, listenerID)
(13) listEventListener(apID)

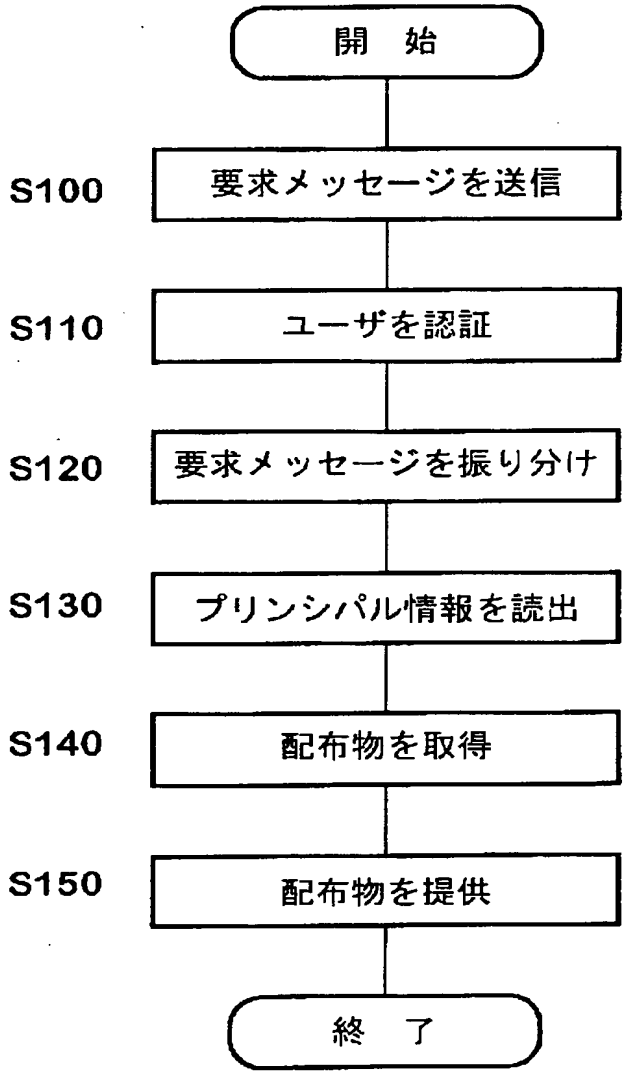
プリンシパル情報管理部内の管理部の動作を示す図

【図４】



オブジェクト情報管理部内の管理部の動作を示す図

【図５】



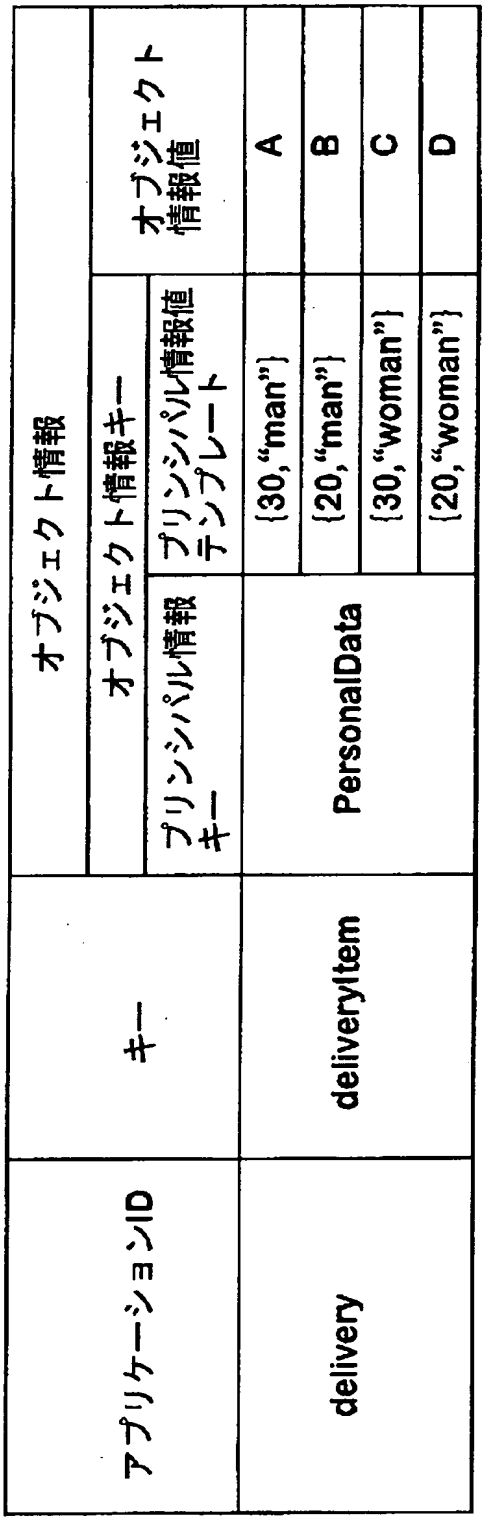
具体例の分散処理システムの動作を示すフローチャート

【図６】

アプリケーションID	プリンシパルID	プリンシパル情報	
		プリンシパル情報キー	プリンシパル情報値
delivery	sakurai123	PersonalData	{1970/1/1,“man”}

プリンシパル情報管理部に記憶された情報を示す図

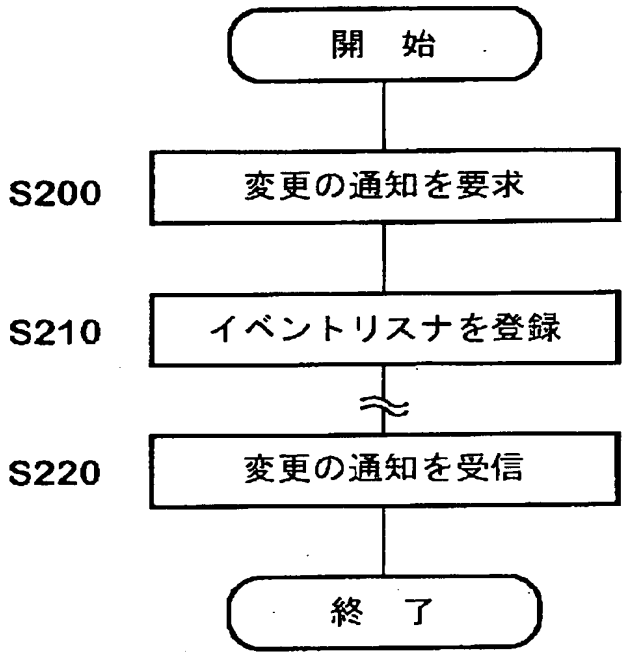
【図７】



アプリケーションID	キー	オブジェクト情報		
		オブジェクト情報キー		オブジェクト情報値
		プリンシパル情報キー	プリンシパル情報値テンプレート	
delivery	deliveryItem	PersonalData	{30,“man”}	A
			{20,“man”}	B
			{30,“woman”}	C
			{20,“woman”}	D

オブジェクト情報管理部に記憶された情報を示す図

【図８】



プリンシパル情報が変更されたときのサービスへの通知を示すフローチャート

【図９】

アプリケーションID	登録リスナ
delivery	listenerA
	listenerB

イベントリスナを管理するテーブルを示す図

【書類名】　　要約書

【要約】

【課題】　従来、アクセス制御リスト等を用いて、プリンシパルによるアクセスを制御することから、アクセス制御の対象となる資源、処理、許否等が限定されていた。

【解決手段】　本発明のオブジェクト提供装置は、プリンシパルに関する情報を記憶するプリンシパル情報記憶部と、プリンシパルに関する情報とオブジェクトとの関係、及びオブジェクトを記憶するオブジェクト情報記憶部と、プリンシパルを認証するための情報をクライアント装置から受信する受信部と、受信したプリンシパルを認証するための情報に基づき、プリンシパルに関する情報を参照することによりプリンシパルを認証する認証部と、認証されたプリンシパルに関する情報を読み出し、プリンシパル情報に対応するオブジェクトを読み出すアプリケーション部とを備える。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－１９８４２０
受付番号	５００００８２４６９１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　７月　３日

＜認定情報・付加情報＞

【提出日】　平成12年 6月30日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２９５〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　　東京都港区虎ノ門１丁目７番１２号
氏　名　　沖電気工業株式会社